TestOut

# TestOut CyberDefense Pro – English 2.0

## Objective Mappings:

TestOut CyberDefense Pro
CompTIA CySA+ CS0-003

Revised: 2023-08-11

Powered by LABSIM

# Contents

This document contains four objective mappings. Click on a mapping to view its contents.

## **Objective Mapping:** LabSim Section to TestOut CyberDefense Pro Objective

| Section | Title | Objectives |
|---|---|---|
| **1.0** | **Introduction** | |
| 1.1 | Introduction to TestOut CyberDefense Pro | |
| **2.0** | **Vulnerability Response, Handling, and Management** | |
| 2.1 | Regulations and Standards | |
| 2.2 | Risk Management | |
| 2.3 | Security Controls | 5.2 Implement physical security controls<br>• 5.2.1 - Analyze physical security design to protect systems |
| 2.4 | Attack Surfaces | 3.1 Implement security controls to mitigate risk<br>• 3.1.7 - Implement and configure a security appliance<br>3.2 Implement system hardening<br>• 3.2.1 - Disable unnecessary services<br>3.4 Implement defensive deception methods<br>• 3.4.3 - Configure a captive portal<br>4.2 Manage devices |

| | | |
|---|---|---|
| | | • 4.2.1 - Secure smartphones, tablets, and laptops |
| 2.5 | Patch Management | 3.1 Implement security controls to mitigate risk<br>• 3.1.1 - Detect unpatched systems<br>3.2 Implement system hardening<br>• 3.2.2 - Check service configuration<br>5.1 Implement Identity and Access Management (IAM)<br>• 5.1.3 - Manage certificates<br>• 5.1.4 - Configure account policies and account control |
| 2.6 | Security Testing | |
| **3.0** | **Threat Intelligence and Threat Hunting** | |
| 3.1 | Threat Actors | 4.1 Manage security incidents<br>• 4.1.2 - Eradicate Advanced Persistent Threats (APT) |
| 3.2 | Threat Intelligence | 2.2 Detect threats using analytics and intelligence<br>• 2.2.1 - Use an Intrusion Detection System (IDS) |
| 3.3 | Threat Hunting | 1.1 Monitor networks<br>• 1.1.1 - Monitor network traffic<br>• 1.1.2 - Monitor network ports and sockets |

| | | |
|---|---|---|
| | | 1.2 Monitor software and systems<br>• 1.2.2 - Analyze executable processes<br>• 1.2.4 - Monitor email for malware<br>1.3 Implement Logging<br>• 1.3.2 - Review event logs<br>• 1.3.4 - Review firewall logs<br>2.1 Perform threat analysis<br>• 2.1.1 - Review firewall configuration<br>• 2.1.3 - Determine the types of vulnerabilities associated with different attacks<br>2.2 Detect threats using analytics and intelligence<br>• 2.2.4 - Check for privilege escalation<br>• 2.2.5 - Perform digital forensics investigations<br>4.1 Manage security incidents<br>• 4.1.2 - Eradicate Advanced Persistent Threats (APT)<br>• 4.1.3 - Respond to Distributed Denial of Service (DDoS) attacks<br>4.3 Analyze Indicators of compromise<br>• 4.3.1 - Examine applications for any signs of compromise<br>• 4.3.2 - Inspect systems for any signs of compromise |

| | | |
|---|---|---|
| | | • 4.3.3 - Investigate networks for any signs of compromise |
| 3.4 | Honeypots | 1.1 Monitor networks<br>• 1.1.1 - Monitor network traffic<br>• 1.1.2 - Monitor network ports and sockets<br>3.1 Implement security controls to mitigate risk<br>• 3.1.3 - Implement anti-virus and endpoint security<br>3.2 Implement system hardening<br>• 3.2.3 - Disable unnecessary ports<br>3.4 Implement defensive deception methods<br>• 3.4.1 - Deploy a honeypot<br>4.1 Manage security incidents<br>• 4.1.1 - Resolve malware, ransomware, and phishing attacks<br>4.3 Analyze Indicators of compromise<br>• 4.3.3 - Investigate networks for any signs of compromise |
| **4.0** | **System and Network Architecture** | |
| 4.1 | Operating System Concepts | 1.2 Monitor software and systems<br>• 1.2.2 - Analyze executable processes |

| | | |
|---|---|---|
| | | 3.2 Implement system hardening<br>• 3.2.1 - Disable unnecessary services<br>• 3.2.2 - Check service configuration<br>4.3 Analyze Indicators of compromise<br>• 4.3.2 - Inspect systems for any signs of compromise |
| 4.2 | Network Architecture | 1.1 Monitor networks<br>• 1.1.1 - Monitor network traffic<br>• 1.1.2 - Monitor network ports and sockets<br>3.1 Implement security controls to mitigate risk<br>• 3.1.5 - Implement cloud security |
| 4.3 | Identity and Access Management (IAM) | 3.1 Implement security controls to mitigate risk<br>• 3.1.5 - Implement cloud security<br>5.1 Implement Identity and Access Management (IAM)<br>• 5.1.1 - Administer user accounts<br>• 5.1.2 - Manage user-based and role-based access<br>• 5.1.4 - Configure account policies and account control |
| 4.4 | Data Protection | 4.2 Manage devices |

| | | |
|---|---|---|
| | | • 4.2.2 - Implement data loss prevention |
| 4.5 | Logging | 1.3 Implement Logging<br>• 1.3.2 - Review event logs<br>• 1.3.3 - Send log events to a remote syslog server<br>• 1.3.4 - Review firewall logs |
| **5.0** | **Vulnerability Assessments** | |
| 5.1 | Reconnaissance | 1.1 Monitor networks<br>• 1.1.1 - Monitor network traffic<br>• 1.1.2 - Monitor network ports and sockets<br>1.2 Monitor software and systems<br>• 1.2.3 - Review web application security<br>3.2 Implement system hardening<br>• 3.2.2 - Check service configuration<br>• 3.2.3 - Disable unnecessary ports<br>3.3 Perform penetration tests<br>• 3.3.1 - Perform internal penetration testing<br>4.1 Manage security incidents |

| | | |
|---|---|---|
| | | • 4.1.3 - Respond to Distributed Denial of Service (DDoS) attacks<br>4.2 Manage devices<br>• 4.2.4 - Secure IOT devices<br>4.3 Analyze Indicators of compromise<br>• 4.3.2 - Inspect systems for any signs of compromise<br>• 4.3.3 - Investigate networks for any signs of compromise |
| 5.2 | Scanning | 1.1 Monitor networks<br>• 1.1.1 - Monitor network traffic<br>• 1.1.2 - Monitor network ports and sockets<br>2.1 Perform threat analysis<br>• 2.1.1 - Review firewall configuration<br>• 2.1.3 - Determine the types of vulnerabilities associated with different attacks<br>2.2 Detect threats using analytics and intelligence<br>• 2.2.1 - Use an Intrusion Detection System (IDS)<br>• 2.2.2 - Use a protocol analyzer and packet analysis to determine threats<br>3.1 Implement security controls to mitigate risk<br>• 3.1.1 - Detect unpatched systems<br>• 3.1.2 - Configure host firewall policies |

| | | |
|---|---|---|
| | | • 3.1.4 - Implement Intrusion Prevention System (IPS)<br>3.2 Implement system hardening<br>• 3.2.3 - Disable unnecessary ports<br>3.3 Perform penetration tests<br>• 3.3.1 - Perform internal penetration testing<br>• 3.3.2 - Perform external penetration testing<br>4.2 Manage devices<br>• 4.2.4 - Secure IOT devices<br>4.3 Analyze Indicators of compromise<br>• 4.3.3 - Investigate networks for any signs of compromise |
| 5.3 | Enumeration | 2.1 Perform threat analysis<br>• 2.1.3 - Determine the types of vulnerabilities associated with different attacks<br>3.3 Perform penetration tests<br>• 3.3.1 - Perform internal penetration testing |
| 5.4 | Vulnerability Assessments | 1.2 Monitor software and systems<br>• 1.2.3 - Review web application security<br>2.1 Perform threat analysis |

| | | |
|---|---|---|
| | | • 2.1.3 - Determine the types of vulnerabilities associated with different attacks<br>3.3 Perform penetration tests<br>• 3.3.2 - Perform external penetration testing<br>4.3 Analyze Indicators of compromise<br>• 4.3.3 - Investigate networks for any signs of compromise |
| 5.5 | Vulnerability Scoring Systems | |
| 5.6 | Classifying Vulnerability Information | 2.1 Perform threat analysis<br>• 2.1.3 - Determine the types of vulnerabilities associated with different attacks<br>3.1 Implement security controls to mitigate risk<br>• 3.1.6 - Perform application and data protection tasks<br>4.3 Analyze Indicators of compromise<br>• 4.3.4 - Analyze indicators for false positives and false negatives |
| **6.0** | **Network Security** | |
| 6.1 | Security Monitoring | 1.1 Monitor networks<br>• 1.1.2 - Monitor network ports and sockets<br>1.3 Implement Logging |

| | | |
|---|---|---|
| | | • 1.3.1 - Manage and perform analysis using Security Information and Event Management (SIEM) tools<br>2.1 Perform threat analysis<br>• 2.1.1 - Review firewall configuration<br>2.2 Detect threats using analytics and intelligence<br>• 2.2.1 - Use an Intrusion Detection System (IDS)<br>• 2.2.3 - Use endpoint protection tools<br>3.2 Implement system hardening<br>• 3.2.2 - Check service configuration |
| 6.2 | Wireless Security | 1.1 Monitor networks<br>• 1.1.2 - Monitor network ports and sockets<br>2.2 Detect threats using analytics and intelligence<br>• 2.2.2 - Use a protocol analyzer and packet analysis to determine threats<br>4.3 Analyze Indicators of compromise<br>• 4.3.3 - Investigate networks for any signs of compromise |
| 6.3 | Web Server Security | 1.2 Monitor software and systems<br>• 1.2.2 - Analyze executable processes<br>• 1.2.3 - Review web application security |

| | | |
|---|---|---|
| 6.4 | SQL Injection | 1.2 Monitor software and systems<br>• 1.2.3 - Review web application security<br>2.1 Perform threat analysis<br>• 2.1.3 - Determine the types of vulnerabilities associated with different attacks |
| 6.5 | Sniffing | 1.1 Monitor networks<br>• 1.1.1 - Monitor network traffic<br>4.3 Analyze Indicators of compromise<br>• 4.3.3 - Investigate networks for any signs of compromise |
| 6.6 | Authentication Attacks | 1.2 Monitor software and systems<br>• 1.2.3 - Review web application security<br>2.1 Perform threat analysis<br>• 2.1.3 - Determine the types of vulnerabilities associated with different attacks<br>4.3 Analyze Indicators of compromise<br>• 4.3.3 - Investigate networks for any signs of compromise<br>5.1 Implement Identity and Access Management (IAM)<br>• 5.1.1 - Administer user accounts |
| 6.7 | Cloud Security | 3.1 Implement security controls to mitigate risk |

| | | |
|---|---|---|
| | | • 3.1.5 - Implement cloud security |
| 6.8 | Email Security | 1.2 Monitor software and systems<br>• 1.2.4 - Monitor email for malware<br>• 1.2.5 - Analyze email headers and impersonation attempts |
| 6.9 | Denial-of-Service Attacks | 1.1 Monitor networks<br>• 1.1.1 - Monitor network traffic<br>4.1 Manage security incidents<br>• 4.1.3 - Respond to Distributed Denial of Service (DDoS) attacks |
| 6.10 | Industrial Computer Systems | |
| **7.0** | **Host-Based Attacks** | |
| 7.1 | Device Security | 1.2 Monitor software and systems<br>• 1.2.1 - Configure execution control and verify digital signatures<br>2.2 Detect threats using analytics and intelligence<br>• 2.2.5 - Perform digital forensics investigations<br>3.2 Implement system hardening<br>• 3.2.1 - Disable unnecessary services |

| | | |
|---|---|---|
| | | 4.2 Manage devices<br>- 4.2.5 - Implement network access control (NAC)<br>5.2 Implement physical security controls<br>- 5.2.3 - Implement drive encryption |
| 7.2 | Unauthorized Changes | 1.2 Monitor software and systems<br>- 1.2.2 - Analyze executable processes<br>2.2 Detect threats using analytics and intelligence<br>- 2.2.4 - Check for privilege escalation<br>3.1 Implement security controls to mitigate risk<br>- 3.1.6 - Perform application and data protection tasks<br>5.1 Implement Identity and Access Management (IAM)<br>- 5.1.4 - Configure account policies and account control |
| 7.3 | Malware | 1.2 Monitor software and systems<br>- 1.2.1 - Configure execution control and verify digital signatures<br>2.1 Perform threat analysis<br>- 2.1.3 - Determine the types of vulnerabilities associated with different attacks |

| | | |
|---|---|---|
| | | 2.2 Detect threats using analytics and intelligence<br>• 2.2.3 - Use endpoint protection tools<br>3.1 Implement security controls to mitigate risk<br>• 3.1.3 - Implement anti-virus and endpoint security<br>4.1 Manage security incidents<br>• 4.1.1 - Resolve malware, ransomware, and phishing attacks<br>4.2 Manage devices<br>• 4.2.1 - Secure smartphones, tablets, and laptops |
| 7.4 | Command and Control | |
| 7.5 | Social Engineering | 1.2 Monitor software and systems<br>• 1.2.4 - Monitor email for malware<br>4.1 Manage security incidents<br>• 4.1.1 - Resolve malware, ransomware, and phishing attacks |
| 7.6 | Scripting and Programming | 4.3 Analyze Indicators of compromise<br>• 4.3.1 - Examine applications for any signs of compromise |
| 7.7 | Application Vulnerabilities | 4.3 Analyze Indicators of compromise |

| | | |
|---|---|---|
| | | • 4.3.1 - Examine applications for any signs of compromise |
| **8.0** | **Security Management** | |
| 8.1 | Security Information and Event Management (SIEM) | 1.1 Monitor networks<br>• 1.1.1 - Monitor network traffic<br>1.3 Implement Logging<br>• 1.3.1 - Manage and perform analysis using Security Information and Event Management (SIEM) tools |
| 8.2 | Security Orchestration, Automation, and Response (SOAR) | |
| 8.3 | Exploring Abnormal Activity | 1.1 Monitor networks<br>• 1.1.2 - Monitor network ports and sockets<br>2.2 Detect threats using analytics and intelligence<br>• 2.2.3 - Use endpoint protection tools<br>3.1 Implement security controls to mitigate risk<br>• 3.1.3 - Implement anti-virus and endpoint security<br>• 3.1.6 - Perform application and data protection tasks<br>4.3 Analyze Indicators of compromise<br>• 4.3.1 - Examine applications for any signs of compromise |

| 9.0 | Post-Attack | |
|---|---|---|
| 9.1 | Containment | 4.1 Manage security incidents<br>• 4.1.2 - Eradicate Advanced Persistent Threats (APT) |
| 9.2 | Incident Response | 2.2 Detect threats using analytics and intelligence<br>• 2.2.3 - Use endpoint protection tools<br>4.1 Manage security incidents<br>• 4.1.1 - Resolve malware, ransomware, and phishing attacks<br>• 4.1.3 - Respond to Distributed Denial of Service (DDoS) attacks<br>4.2 Manage devices<br>• 4.2.2 - Implement data loss prevention<br>4.3 Analyze Indicators of compromise<br>• 4.3.2 - Inspect systems for any signs of compromise |
| 9.3 | Post-Incident Activities | 2.2 Detect threats using analytics and intelligence<br>• 2.2.5 - Perform digital forensics investigations<br>4.2 Manage devices<br>• 4.2.2 - Implement data loss prevention |
| A.0 | CompTIA CySA+ CS0-003 - Practice Exams | |

| | | |
|---|---|---|
| A.1 | Prepare for CompTIA CySA+ Certification | |
| A.2 | CompTIA CySA+ CS0-003 Domain Review (20 Questions) | |
| A.3 | CompTIA CySA+ CS0-003 Practice Exams (All Questions) | |
| **B.0** | **TestOut CyberDefense Pro - Practice Exams** | |
| B.1 | Prepare for TestOut CyberDefense Pro Certification | |
| B.2 | TestOut CyberDefense Pro Exam Domain Review | |

## **Objective Mapping:** TestOut CyberDefense Pro Objective to LabSim Section

| # | Domain | Module.Section |
|---|---|---|
| **1.0** | **Monitoring and Log Analysis** | |
| 1.1 | Monitor networks<br>1.1.1 - Monitor network traffic<br>1.1.2 - Monitor network ports and sockets | 3.3, 3.4<br>4.2<br>5.1, 5.2<br>6.1, 6.2, 6.5, 6.9<br>8.1, 8.3 |
| 1.2 | Monitor software and systems<br>1.2.1 - Configure execution control and verify digital signatures<br>1.2.2 - Analyze executable processes<br>1.2.3 - Review web application security<br>1.2.4 - Monitor email for malware<br>1.2.5 - Analyze email headers and impersonation attempts | 3.3<br>4.1<br>5.1, 5.4<br>6.3, 6.4, 6.6, 6.8<br>7.1, 7.2, 7.3, 7.5 |
| 1.3 | Implement Logging<br>1.3.1 - Manage and perform analysis using Security Information and Event Management (SIEM) tools<br>1.3.2 - Review event logs<br>1.3.3 - Send log events to a remote syslog server<br>1.3.4 - Review firewall logs | 3.3<br>4.5<br>6.1<br>8.1 |
| **2.0** | **Threat Analysis and Detection** | |
| 2.1 | Perform threat analysis<br>2.1.1 - Review firewall configuration | 3.3<br>5.2, 5.3, 5.4, 5.6 |

| | | |
|---|---|---|
| | 2.1.2 - Conduct a trend analysis<br>2.1.3 - Determine the types of vulnerabilities associated with different attacks | 6.1, 6.4, 6.6<br>7.3 |
| 2.2 | Detect threats using analytics and intelligence<br>2.2.1 - Use an Intrusion Detection System (IDS)<br>2.2.2 - Use a protocol analyzer and packet analysis to determine threats<br>2.2.3 - Use endpoint protection tools<br>2.2.4 - Check for privilege escalation<br>2.2.5 - Perform digital forensics investigations | 3.2, 3.3<br>5.2<br>6.1, 6.2<br>7.1, 7.2, 7.3<br>8.3<br>9.2, 9.3 |
| **3.0** | **Risk Analysis and Mitigation** | |
| 3.1 | Implement security controls to mitigate risk<br>3.1.1 - Detect unpatched systems<br>3.1.2 - Configure host firewall policies<br>3.1.3 - Implement anti-virus and endpoint security<br>3.1.4 - Implement Intrusion Prevention System (IPS)<br>3.1.5 - Implement cloud security<br>3.1.6 - Perform application and data protection tasks<br>3.1.7 - Implement and configure a security appliance | 2.4, 2.5<br>3.4<br>4.2, 4.3<br>5.2, 5.6<br>6.7<br>7.2, 7.3<br>8.3 |
| 3.2 | Implement system hardening<br>3.2.1 - Disable unnecessary services<br>3.2.2 - Check service configuration<br>3.2.3 - Disable unnecessary ports | 2.4, 2.5<br>3.4<br>4.1<br>5.1, 5.2<br>6.1 |

| | | |
|---|---|---|
| | | 7.1 |
| 3.3 | Perform penetration tests<br>3.3.1 - Perform internal penetration testing<br>3.3.2 - Perform external penetration testing | 3.3<br>5.1, 5.2, 5.3, 5.4 |
| 3.4 | Implement defensive deception methods<br>3.4.1 - Deploy a honeypot<br>3.4.2 - Implement a black hole or sinkhole<br>3.4.3 - Configure a captive portal | 2.4<br>3.4 |
| **4.0** | **Incident Response** | |
| 4.1 | Manage security incidents<br>4.1.1 - Resolve malware, ransomware, and phishing attacks<br>4.1.2 - Eradicate Advanced Persistent Threats (APT)<br>4.1.3 - Respond to Distributed Denial of Service (DDoS) attacks | 3.1, 3.3, 3.4<br>5.1<br>6.9<br>7.3, 7.5<br>9.1, 9.2 |
| 4.2 | Manage devices<br>4.2.1 - Secure smartphones, tablets, and laptops<br>4.2.2 - Implement data loss prevention<br>4.2.3 - Secure embedded devices<br>4.2.4 - Secure IOT devices<br>4.2.5 - Implement network access control (NAC) | 2.4<br>4.4<br>5.1, 5.2<br>7.1, 7.3<br>9.2, 9.3 |
| 4.3 | Analyze Indicators of compromise | 3.3, 3.4<br>4.1 |

| | | |
|---|---|---|
| | 4.3.1 - Examine applications for any signs of compromise<br>4.3.2 - Inspect systems for any signs of compromise<br>4.3.3 - Investigate networks for any signs of compromise<br>4.3.4 - Analyze indicators for false positives and false negatives | 5.1, 5.2, 5.4, 5.6<br>6.2, 6.5, 6.6<br>7.6, 7.7<br>8.3<br>9.2 |
| **5.0** | **Audit and Compliance** | |
| 5.1 | Implement Identity and Access Management (IAM)<br>5.1.1 - Administer user accounts<br>5.1.2 - Manage user-based and role-based access<br>5.1.3 - Manage certificates<br>5.1.4 - Configure account policies and account control | 1.1, 2.5<br>4.3<br>6.6<br>7.2 |
| 5.2 | Implement physical security controls<br>5.2.1 - Analyze physical security design to protect systems<br>5.2.2 - Analyze system security design to protect systems<br>5.2.3 - Implement drive encryption<br>5.2.4 - Implement physical access controls | 2.3<br>7.1 |

## **Objective Mapping:** LabSim Section to CompTIA CySA+ CS0-003 Objective

| Section | Title | Objectives |
|---|---|---|
| **1.0** | **Introduction** | |
| 1.1 | Introduction to TestOut CyberDefense Pro | |
| **2.0** | **Vulnerability Response, Handling, and Management** | |
| 2.1 | Regulations and Standards | 2.1 Given a scenario, implement vulnerability scanning methods and concepts<br>• 2.1.10 - Industry frameworks<br>2.1.10.1 - Payment Card Industry Data Security Standard (PCI DSS)<br>2.1.10.2 - Center for Internet Security (CIS) benchmarks<br>2.1.10.3 - Open Web Application Security Project (OWASP)<br>2.1.10.4 - International Organization for Standardization (ISO) 27000 series<br>2.5 Explain concepts related to vulnerability response, handling, and management<br>• 2.5.6 - Risk management principles<br>2.5.6.3 - Avoid<br>2.5.6.4 - Mitigate<br>• 2.5.7 - Policies, governance, and service-level objectives (SLOs)<br>4.1 Explain the importance of vulnerability management reporting and communication<br>• 4.1.5 - Metrics and key performance indicators (KPIs) |

| | | |
|---|---|---|
| | | 4.1.5.4 - SLOs |
| 2.2 | Risk Management | 1.4 Compare and contrast threat-intelligence and threat-hunting concepts<br>• 1.4.5 - Threat intelligence sharing<br>1.4.5.3 - Risk management<br>2.5 Explain concepts related to vulnerability response, handling, and management<br>• 2.5.6 - Risk management principles<br>2.5.6.1 - Accept<br>2.5.6.2 - Transfer<br>2.5.6.3 - Avoid<br>2.5.6.4 - Mitigate<br>• 2.5.12 - Threat modeling |
| 2.3 | Security Controls | 2.1 Given a scenario, implement vulnerability scanning methods and concepts<br>• 2.1.10 - Industry frameworks<br>2.5 Explain concepts related to vulnerability response, handling, and management<br>• 2.5.1 - Compensating control<br>• 2.5.2 - Control types<br>2.5.2.1 - Managerial<br>2.5.2.2 - Operational<br>2.5.2.3 - Technical<br>2.5.2.4 - Preventative<br>2.5.2.5 - Detective<br>2.5.2.6 - Responsive |

| | | |
|---|---|---|
| | | 2.5.2.7 - Corrective<br>• 2.5.8 - Prioritization and escalation<br>• 2.5.9 - Attack surface management<br>2.5.9.3 - Security controls testing |
| 2.4 | Attack Surfaces | 1.4 Compare and contrast threat-intelligence and threat-hunting concepts<br>• 1.4.6 - Threat hunting<br>1.4.6.3 - Active defense<br>2.5 Explain concepts related to vulnerability response, handling, and management<br>• 2.5.9 - Attack surface management<br>2.5.9.1 - Edge discovery<br>2.5.9.2 - Passive discovery<br>2.5.9.3 - Security controls testing<br>2.5.9.4 - Penetration testing and adversary emulation<br>2.5.9.5 - Bug bounty<br>2.5.9.6 - Attack surface reduction |
| 2.5 | Patch Management | 2.5 Explain concepts related to vulnerability response, handling, and management<br>• 2.5.3 - Patching and configuration management<br>• 2.5.3.1 - Testing<br>• 2.5.3.2 - Implementation<br>• 2.5.3.3 - Rollback<br>• 2.5.4 - Maintenance windows |

| | | |
|---|---|---|
| | | 4.1 Explain the importance of vulnerability management reporting and communication<br>• 4.1.3 - Action plans<br>4.1.3.2 - Patching |
| 2.6 | Security Testing | 1.4 Compare and contrast threat-intelligence and threat-hunting concepts<br>• 1.4.1 - Threat actors<br>3.1 Explain concepts related to attack methodology frameworks<br>• 3.1.1 - Cyber kill chain<br>3.1.1.1 - Reconnaissance<br>3.1.1.2 - Weaponization<br>3.1.1.3 - Delivery<br>3.1.1.4 - Exploitation<br>3.1.1.5 - Installation<br>3.1.1.6 - Command and Control (C2)<br>3.1.1.7 - Actions and objectives<br>• 3.1.2 - Diamond Model of Intrusion Analysis<br>3.1.2.1 - Adversary<br>3.1.2.2 - Victim<br>3.1.2.3 - Infrastructure<br>3.1.2.4 - Capability<br>• 3.1.3 - MITRE ATT&CK<br>• 3.1.4 - Open Source Security Testing Methodology Manual (OSS TMM) |
| **3.0** | **Threat Intelligence and Threat Hunting** | |

| | | |
|---|---|---|
| 3.1 | Threat Actors | 1.4 Compare and contrast threat-intelligence and threat-hunting concepts<br>• 1.4.1 - Threat actors<br>1.4.1.1 - Advanced persistent threat (APT)<br>1.4.1.2 - Hacktivists<br>1.4.1.3 - Organized crime<br>1.4.1.4 - Nation-state<br>1.4.1.5 - Script kiddie<br>1.4.1.6 - Insider threat<br>1.4.1.6.1 - Intentional<br>1.4.1.6.2 - Unintentional<br>1.4.1.7 - Supply chain |
| 3.2 | Threat Intelligence | 1.2 Given a scenario, analyze indicators of potentially malicious activity<br>• 1.2.1 - Network-related<br>1.2.1.5 - Scans/sweep<br>1.4 Compare and contrast threat-intelligence and threat-hunting concepts<br>• 1.4.3 - Confidence levels<br>1.4.3.1 - Timeliness<br>1.4.3.2 - Relevancy<br>1.4.3.3 - Accuracy<br>• 1.4.4 - Collection methods and sources<br>1.4.4.1 - Open source<br>1.4.4.1.2 - Blogs/forums<br>1.4.4.1.3 - Government bulletins<br>1.4.4.1.4 - Computer emergency response team (CERT)<br>1.4.4.1.5 - Cybersecurity incident response team (CSIRT)<br>1.4.4.1.6 - Deep/dark web |

| | | |
|---|---|---|
| | | 1.4.4.2 - Closed source<br>1.4.4.2.1 - Paid feeds<br>1.4.4.2.2 - Information sharing organizations<br>1.4.4.2.3 - Internal sources<br>• 1.4.5 - Threat intelligence sharing<br>1.4.5.1 - Incident response<br>1.4.5.2 - Vulnerability management<br>1.4.5.3 - Risk management<br>1.4.5.4 - Security engineering<br>1.4.5.5 - Detection and monitoring<br>2.1 Given a scenario, implement vulnerability scanning methods and concepts<br>• 2.1.6 - Passive vs. active<br>• 2.1.8 - Critical infrastructure |
| 3.3 | Threat Hunting | 1.2 Given a scenario, analyze indicators of potentially malicious activity<br>• 1.2.1 - Network-related<br>1.2.1.1 - Bandwidth consumption<br>1.2.1.3 - Irregular peer-to-peer communication<br>1.2.1.7 - Activity on unexpected ports<br>• 1.2.2 - Host-related<br>1.2.2.1 - Processor consumption<br>1.2.2.2 - Memory consumption<br>1.2.2.3 - Drive capacity consumption<br>1.2.2.7 - Unauthorized privileges<br>1.2.2.10 - File system changes or anomalies<br>1.2.2.11 - Registry changes or anomalies |

| | | |
|---|---|---|
| | | • 1.2.3 - Application-related<br>1.2.3.1 - Anomalous activity<br>1.4 Compare and contrast threat-intelligence and threat-hunting concepts<br>• 1.4.1 - Threat actors<br>1.4.1.1 - Advanced persistent threat (APT)<br>• 1.4.2 - Tactics, techniques, and procedures (TTP)<br>• 1.4.5 - Threat intelligence sharing<br>1.4.5.5 - Detection and monitoring<br>• 1.4.6 - Threat hunting<br>1.4.6.1 - Indicators of compromise (IoC)<br>1.4.6.1.1 - Collection<br>1.4.6.1.2 - Analysis<br>1.4.6.1.3 - Application<br>1.4.6.2 - Focus areas<br>1.4.6.2.1 - Configurations/ misconfigurations<br>1.4.6.2.2 - Isolated networks<br>1.4.6.2.3 - Business-critical assets and processes<br>1.5 Explain the importance of efficiency and process improvement in security operations<br>• 1.5.2 - Streamline operations<br>1.5.2.2 - Orchestrating threat intelligence data<br>2.5 Explain concepts related to vulnerability response, handling, and management |

| | | |
|---|---|---|
| | | • 2.5.9 - Attack surface management<br>2.5.9.6 - Attack surface reduction<br>• 2.5.12 - Threat modeling<br>3.1 Explain concepts related to attack methodology frameworks<br>• 3.1.3 - MITRE ATT&CK<br>3.2 Given a scenario, perform incident response activities<br>• 3.2.1 - Detection and analysis<br>3.2.1.1 - IoC<br>3.2.1.3 - Data and log analysis<br>3.3 Explain the preparation and post-incident activity phases of the incident management life cycle<br>• 3.3.2 - Post-incident activity<br>3.3.2.1 - Forensic analysis |
| 3.4 | Honeypots | 1.2 Given a scenario, analyze indicators of potentially malicious activity<br>• 1.2.1 - Network-related<br>1.2.1.5 - Scans/sweep<br>• 1.2.2 - Host-related<br>1.2.2.5 - Malicious processes |

| | | |
|---|---|---|
| | | • 1.2.3 - Application-related<br>1.2.3.4 - Unexpected outbound communication<br>1.4 Compare and contrast threat-intelligence and threat-hunting concepts<br>• 1.4.1 - Threat actors<br>• 1.4.6 - Threat hunting<br>1.4.6.3 - Active defense<br>1.4.6.4 - Honeypot<br>2.1 Given a scenario, implement vulnerability scanning methods and concepts<br>• 2.1.3 - Internal vs. external scanning<br>• 2.1.9 - Security baseline scanning<br>2.2 Given a scenario, analyze output from vulnerability assessment tools<br>• 2.2.1 - Tools<br>2.2.1.1 - Network scanning and mapping<br>2.3 Given a scenario, analyze data to prioritize vulnerabilities<br>• 2.3.1 - Common Vulnerability Scoring System (CVSS) interpretation<br>2.3.1.6.2 - Integrity<br>2.5 Explain concepts related to vulnerability response, handling, and management<br>• 2.5.9 - Attack surface management |

| | | |
|---|---|---|
| | | 2.5.9.4 - Penetration testing and adversary emulation<br>3.2 Given a scenario, perform incident response activities<br>• 3.2.1 - Detection and analysis<br>3.2.1.3 - Data and log analysis |
| **4.0** | **System and Network Architecture** | |
| 4.1 | Operating System Concepts | 1.1 Explain the importance of system and network architecture concepts in security operations<br>• 1.1.2 - Operating system (OS) concepts<br>1.1.2.1 - Windows Registry<br>1.1.2.2 - System hardening<br>1.1.2.3 - File structure<br>1.1.2.3.1 - Configuration file locations<br>1.1.2.4 - System processes<br>1.1.2.5 - Hardware architecture<br>1.2 Given a scenario, analyze indicators of potentially malicious activity<br>• 1.2.1 - Network-related<br>1.2.1.5 - Scans/sweep<br>2.1 Given a scenario, implement vulnerability scanning methods and concepts<br>• 2.1.10 - Industry frameworks<br>2.1.10.2 - Center for Internet Security (CIS) benchmarks |

| | | |
|---|---|---|
| | | 2.2 Given a scenario, analyze output from vulnerability assessment tools<br>• 2.2.1 - Tools<br>2.2.1.5.1 - Nmap |
| 4.2 | Network Architecture | 1.1 Explain the importance of system and network architecture concepts in security operations<br>• 1.1.3 - Infrastructure concepts<br>1.1.3.1 - Serverless<br>1.1.3.2 - Virtualization<br>1.1.3.3 - Containerization<br>• 1.1.4 - Network architecture<br>1.1.4.1 - On-premises<br>1.1.4.2 - Cloud<br>1.1.4.3 - Hybrid<br>1.1.4.5 - Zero trust<br>1.1.4.6 - Secure access secure edge (SASE)<br>1.1.4.7 - Software-defined networking (SDN)<br>1.4 Compare and contrast threat-intelligence and threat-hunting concepts<br>• 1.4.6 - Threat hunting<br>1.4.6.3 - Active defense |
| 4.3 | Identity and Access Management (IAM) | 1.1 Explain the importance of system and network architecture concepts in security operations<br>• 1.1.5 - Identity and access management |

| | | |
|---|---|---|
| | | 1.1.5.1 - Multifactor authentication (MFA)<br>1.1.5.2 - Single sign-on (SSO)<br>1.1.5.3 - Federation<br>1.1.5.4 - Privileged access management (PAM)<br>1.1.5.5 - Passwordless<br>1.1.5.6 - Cloud access security broker (CASB) |
| 4.4 | Data Protection | 1.1 Explain the importance of system and network architecture concepts in security operations<br>• 1.1.6 - Encryption<br>1.1.6.1 - Public key infrastructure (PKI)<br>1.1.6.2 - Secure sockets layer (SSL) inspection<br>• 1.1.7 - Sensitive data protection<br>1.1.7.1 - Data loss prevention (DLP)<br>1.1.7.2 - Personally identifiable information (PII)<br>1.1.7.3 - Cardholder data (CHD)<br>1.2 Given a scenario, analyze indicators of potentially malicious activity<br>• 1.2.2 - Host-related<br>1.2.2.2 - Memory consumption<br>1.2.2.8 - Data exfiltration<br>1.2.2.10 - File system changes or anomalies<br>1.3 Given a scenario, use appropriate tools or techniques to determine malicious activity<br>• 1.3.1 - Tools |

| | | |
|---|---|---|
| | | 1.3.1.1 - Packet capture<br>• 1.3.2 - Common techniques<br>1.3.2.5 - User behavior analysis<br>1.4 Compare and contrast threat-intelligence and threat-hunting concepts<br>• 1.4.5 - Threat intelligence sharing<br>1.4.5.2 - Vulnerability management<br>1.4.5.5 - Detection and monitoring<br>2.1 Given a scenario, implement vulnerability scanning methods and concepts<br>• 2.1.1 - Asset discovery<br>2.3 Given a scenario, analyze data to prioritize vulnerabilities<br>• 2.3.1 - Common Vulnerability Scoring System (CVSS) interpretation<br>2.3.1.6 - Impact<br>2.3.1.6.1 - Confidentiality<br>2.3.1.6.2 - Integrity<br>2.3.1.6.3 - Availability<br>4.1 Explain the importance of vulnerability management reporting and communication<br>• 4.1.5 - Metrics and key performance indicators (KPIs)<br>4.1.5.1 - Trends |

| | | |
|---|---|---|
| 4.5 | Logging | 1.1 Explain the importance of system and network architecture concepts in security operations<br>• 1.1.1 - Log ingestion<br>1.1.1.1 - Time synchronization<br>1.1.1.2 - Logging levels<br>1.2 Given a scenario, analyze indicators of potentially malicious activity<br>• 1.2.3 - Application-related<br>1.2.3.6 - Application logs<br>1.3 Given a scenario, use appropriate tools or techniques to determine malicious activity<br>• 1.3.1 - Tools<br>1.3.1.2 - Log analysis/correlation<br>3.2 Given a scenario, perform incident response activities<br>• 3.2.1 - Detection and analysis<br>3.2.1.3 - Data and log analysis |
| **5.0** | **Vulnerability Assessments** | |
| 5.1 | Reconnaissance | 1.1 Explain the importance of system and network architecture concepts in security operations<br>• 1.1.2 - Operating system (OS) concepts |

| | | |
|---|---|---|
| | | 1.1.2.2 - System hardening<br>1.2 Given a scenario, analyze indicators of potentially malicious activity<br>• 1.2.1 - Network-related<br>1.2.1.1 - Bandwidth consumption<br>1.2.1.4 - Rogue devices on the network<br>1.2.1.5 - Scans/sweep<br>1.2.1.6 - Unusual traffic spikes<br>1.3 Given a scenario, use appropriate tools or techniques to determine malicious activity<br>• 1.3.1 - Tools<br>1.3.1.1.1 - Wireshark<br>1.3.1.4 - Domain name service (DNS) and Internet Protocol (IP) reputation<br>1.3.1.4.1 - WHOIS<br>• 1.3.3 - Programming languages/scripting<br>1.3.3.4 - PowerShell<br>2.1 Given a scenario, implement vulnerability scanning methods and concepts<br>• 2.1.1 - Asset discovery<br>2.1.1.2 - Device fingerprinting<br>• 2.1.3 - Internal vs. external scanning<br>• 2.1.6 - Passive vs. active |

| | | |
|---|---|---|
| | | • 2.1.10 - Industry frameworks<br>2.1.10.3 - Open Web Application Security Project (OWASP)<br>2.2 Given a scenario, analyze output from vulnerability assessment tools<br>• 2.2.1 - Tools<br>2.2.1.1 - Network scanning and mapping<br>2.2.1.1.2 - Maltego<br>2.2.1.2 - Web application scanners<br>2.2.1.2.2 - Zed Attack Proxy (ZAP)<br>2.2.1.5 - Multipurpose<br>2.2.1.5.1 - Nmap<br>2.2.1.5.2 - Metasploit framework (MSF)<br>2.2.1.5.3 - Recon-ng<br>2.4 Given a scenario, recommend controls to mitigate attacks and software vulnerabilities<br>• 2.4.2 - Overflow vulnerabilities<br>2.4.2.1 - Buffer<br>3.2 Given a scenario, perform incident response activities<br>• 3.2.1 - Detection and analysis<br>3.2.1.3 - Data and log analysis |
| 5.2 | Scanning | 1.1 Explain the importance of system and network architecture concepts in security operations<br>• 1.1.4 - Network architecture |

| | | |
|---|---|---|
| | | 1.1.4.5 - Zero trust<br>1.2 Given a scenario, analyze indicators of potentially malicious activity<br>• 1.2.1 - Network-related<br>1.2.1.1 - Bandwidth consumption<br>1.2.1.4 - Rogue devices on the network<br>1.2.1.5 - Scans/sweep<br>1.2.1.7 - Activity on unexpected ports<br>• 1.2.3 - Application-related<br>1.2.3.1 - Anomalous activity<br>1.4 Compare and contrast threat-intelligence and threat-hunting concepts<br>• 1.4.2 - Tactics, techniques, and procedures (TTP)<br>• 1.4.6 - Threat hunting<br>1.4.6.2.1 - Configurations/ misconfigurations<br>1.4.6.3 - Active defense<br>2.1 Given a scenario, implement vulnerability scanning methods and concepts<br>• 2.1.1 - Asset discovery<br>2.1.1.1 - Map scans<br>2.1.1.2 - Device fingerprinting<br>• 2.1.2 - Special considerations<br>2.1.2.1 - Scheduling<br>2.1.2.2 - Operations |

| | | |
|---|---|---|
| | | 2.1.2.3 - Performance<br>2.1.2.4 - Sensitivity levels<br>2.1.2.5 - Segmentation<br>2.1.2.6 - Regulatory requirements<br>• 2.1.3 - Internal vs. external scanning<br>• 2.1.4 - Agent vs. agentless<br>• 2.1.5 - Credentialed vs. non-credentialed<br>• 2.1.6 - Passive vs. active<br>2.2 Given a scenario, analyze output from vulnerability assessment tools<br>• 2.2.1 - Tools<br>2.2.1.1 - Network scanning and mapping<br>2.2.1.1.1 - Angry IP Scanner<br>2.2.1.1.2 - Maltego<br>2.2.1.3 - Vulnerability scanners<br>2.2.1.3.1 - Nessus<br>2.2.1.3.2 - OpenVAS<br>2.2.1.5.1 - Nmap<br>2.2.1.5.2 - Metasploit framework (MSF)<br>2.2.1.5.3 - Recon-ng<br>2.3 Given a scenario, analyze data to prioritize vulnerabilities<br>• 2.3.1 - Common Vulnerability Scoring System (CVSS) interpretation<br>2.3.1.6.3 - Availability<br>• 2.3.2 - Validation<br>2.3.2.1 - True/false positives |

| | | |
|---|---|---|
| | | 2.5 Explain concepts related to vulnerability response, handling, and management<br>• 2.5.9 - Attack surface management<br>2.5.9.4 - Penetration testing and adversary emulation<br>3.2 Given a scenario, perform incident response activities<br>• 3.2.2 - Containment, eradication, and recovery<br>3.2.2.1 - Scope |
| 5.3 | Enumeration | 2.1 Given a scenario, implement vulnerability scanning methods and concepts<br>• 2.1.1 - Asset discovery<br>2.1.1.1 - Map scans<br>2.1.1.2 - Device fingerprinting<br>• 2.1.2 - Special considerations<br>2.1.2.3 - Performance<br>2.1.2.6 - Regulatory requirements<br>• 2.1.6 - Passive vs. active<br>• 2.1.7 - Static vs. dynamic<br>2.1.7.1 - Reverse engineering<br>2.1.7.2 - Fuzzing<br>2.2 Given a scenario, analyze output from vulnerability assessment tools<br>• 2.2.1 - Tools |

| | | |
|---|---|---|
| | | 2.2.1.5.1 - Nmap<br>2.2.1.5.2 - Metasploit framework (MSF)<br>2.4 Given a scenario, recommend controls to mitigate attacks and software vulnerabilities<br>• 2.4.10 - Security misconfiguration<br>2.5 Explain concepts related to vulnerability response, handling, and management<br>• 2.5.9 - Attack surface management<br>2.5.9.4 - Penetration testing and adversary emulation |
| 5.4 | Vulnerability Assessments | 2.1 Given a scenario, implement vulnerability scanning methods and concepts<br>• 2.1.5 - Credentialed vs. non-credentialed<br>• 2.1.7 - Static vs. dynamic<br>2.1.7.2 - Fuzzing<br>2.2 Given a scenario, analyze output from vulnerability assessment tools<br>• 2.2.1 - Tools<br>2.2.1.2.1 - Burp Suite<br>2.2.1.2.2 - Zed Attack Proxy (ZAP)<br>2.2.1.2.3 - Arachni<br>2.2.1.2.4 - Nikto<br>2.2.1.3 - Vulnerability scanners<br>2.2.1.3.1 - Nessus<br>2.2.1.3.2 - OpenVAS |

| | | |
|---|---|---|
| | | 2.3 Given a scenario, analyze data to prioritize vulnerabilities<br>• 2.3.1 - Common Vulnerability Scoring System (CVSS) interpretation<br>2.4 Given a scenario, recommend controls to mitigate attacks and software vulnerabilities<br>• 2.4.1 - Cross-site scripting<br>• 2.4.6 - Injection flaws<br>• 2.4.7 - Cross-site request forgery<br>• 2.4.16 - Local file inclusion (LFI)/remote file inclusion (RFI)<br>2.5 Explain concepts related to vulnerability response, handling, and management<br>• 2.5.9 - Attack surface management<br>2.5.9.3 - Security controls testing<br>2.5.9.4 - Penetration testing and adversary emulation<br>4.1 Explain the importance of vulnerability management reporting and communication<br>• 4.1.1 - Vulnerability management reporting<br>4.1.1.1 - Vulnerabilities<br>4.1.1.3 - Risk score<br>4.1.1.4 - Mitigation |
| 5.5 | Vulnerability Scoring Systems | 1.4 Compare and contrast threat-intelligence and threat-hunting concepts<br>• 1.4.4 - Collection methods and sources<br>1.4.4.1 - Open source |

| | | |
|---|---|---|
| | | 1.4.4.1.2 - Blogs/forums<br>1.4.4.1.3 - Government bulletins<br>• 1.4.5 - Threat intelligence sharing<br>1.4.5.2 - Vulnerability management<br>2.2 Given a scenario, analyze output from vulnerability assessment tools<br>• 2.2.1 - Tools<br>2.2.1.3.1 - Nessus<br>2.2.1.3.2 - OpenVAS<br>2.3 Given a scenario, analyze data to prioritize vulnerabilities<br>• 2.3.1 - Common Vulnerability Scoring System (CVSS) interpretation<br>2.3.1.1 - Attack vectors<br>2.3.1.2 - Attack complexity<br>2.3.1.3 - Privileges required<br>2.3.1.4 - User interaction<br>2.3.1.5 - Scope<br>2.3.1.6 - Impact<br>2.3.1.6.1 - Confidentiality<br>2.3.1.6.2 - Integrity<br>2.3.1.6.3 - Availability<br>• 2.3.4 - Exploitability/weaponization<br>• 2.3.5 - Asset value<br>• 2.3.6 - Zero-day<br>4.1 Explain the importance of vulnerability management reporting and communication |

| | | |
|---|---|---|
| | | • 4.1.1 - Vulnerability management reporting<br>4.1.1.1 - Vulnerabilities<br>4.1.1.3 - Risk score |
| 5.6 | Classifying Vulnerability Information | 1.4 Compare and contrast threat-intelligence and threat-hunting concepts<br>• 1.4.4 - Collection methods and sources<br>1.4.4.1.3 - Government bulletins<br>2.1 Given a scenario, implement vulnerability scanning methods and concepts<br>• 2.1.1 - Asset discovery<br>• 2.1.2 - Special considerations<br>2.1.2.6 - Regulatory requirements<br>• 2.1.9 - Security baseline scanning<br>• 2.1.10 - Industry frameworks<br>2.1.10.2 - Center for Internet Security (CIS) benchmarks<br>2.3 Given a scenario, analyze data to prioritize vulnerabilities<br>• 2.3.2 - Validation<br>2.3.2.1 - True/false positives<br>2.3.2.2 - True/false negatives<br>2.5 Explain concepts related to vulnerability response, handling, and management<br>• 2.5.3.1 - Testing |

| | | |
|---|---|---|
| | | • 2.5.3.2 - Implementation<br>• 2.5.3.4 - Validation<br>• 2.5.6 - Risk management principles<br>• 2.5.7 - Policies, governance, and service-level objectives (SLOs)<br>• 2.5.8 - Prioritization and escalation<br>4.1 Explain the importance of vulnerability management reporting and communication<br>• 4.1.1 - Vulnerability management reporting<br>4.1.1.1 - Vulnerabilities<br>4.1.1.2 - Affected hosts<br>4.1.1.3 - Risk score<br>4.1.1.4 - Mitigation<br>4.1.1.5 - Recurrence<br>4.1.1.6 - Prioritization<br>• 4.1.2 - Compliance reports<br>• 4.1.3 - Action plans<br>4.1.3.1 - Configuration management<br>4.1.3.2 - Patching<br>4.1.3.3 - Compensating controls<br>4.1.3.4 - Awareness, education, and training<br>4.1.3.5 - Changing business requirements<br>• 4.1.4 - Inhibitors to remediation<br>4.1.4.1 - Memorandum of understanding (MOU)<br>4.1.4.2 - Service-level agreement (SLA)<br>4.1.4.3 - Organizational governance<br>4.1.4.4 - Business process interruption<br>4.1.4.5 - Degrading functionality |

| | | |
|---|---|---|
| | | 4.1.4.6 - Legacy systems<br>4.1.4.7 - Proprietary systems<br>• 4.1.5 - Metrics and key performance indicators (KPIs)<br>4.1.5.2 - Top 10<br>4.1.5.4 - SLOs<br>• 4.1.6 - Stakeholder identification and communication |
| **6.0** | **Network Security** | |
| 6.1 | Security Monitoring | 1.2 Given a scenario, analyze indicators of potentially malicious activity<br>• 1.2.1 - Network-related<br>• 1.2.4 - Other<br>1.2.4.2 - Obfuscated links<br>1.4 Compare and contrast threat-intelligence and threat-hunting concepts<br>• 1.4.5 - Threat intelligence sharing<br>1.4.5.5 - Detection and monitoring<br>2.1 Given a scenario, implement vulnerability scanning methods and concepts<br>• 2.1.2 - Special considerations<br>2.1.2.5 - Segmentation<br>2.2 Given a scenario, analyze output from vulnerability assessment tools<br>• 2.2.1 - Tools |

| | | |
|---|---|---|
| | | 2.2.1.1 - Network scanning and mapping<br>2.2.1.5.1 - Nmap<br>3.2 Given a scenario, perform incident response activities<br>• 3.2.1 - Detection and analysis<br>4.1 Explain the importance of vulnerability management reporting and communication<br>• 4.1.5 - Metrics and key performance indicators (KPIs)<br>4.1.5.1 - Trends |
| 6.2 | Wireless Security | 1.2 Given a scenario, analyze indicators of potentially malicious activity<br>• 1.2.1 - Network-related<br>1.2.1.4 - Rogue devices on the network<br>1.2.1.7 - Activity on unexpected ports |
| 6.3 | Web Server Security | 1.2 Given a scenario, analyze indicators of potentially malicious activity<br>• 1.2.1 - Network-related<br>1.3 Given a scenario, use appropriate tools or techniques to determine malicious activity<br>• 1.3.1 - Tools<br>1.3.1.4 - Domain name service (DNS) and Internet Protocol (IP) reputation |

| | | |
|---|---|---|
| | | 2.2 Given a scenario, analyze output from vulnerability assessment tools<br>• 2.2.1 - Tools<br>2.2.1.1 - Network scanning and mapping<br>2.2.1.2 - Web application scanners<br>2.4 Given a scenario, recommend controls to mitigate attacks and software vulnerabilities<br>• 2.4.1 - Cross-site scripting<br>• 2.4.2 - Overflow vulnerabilities<br>• 2.4.3 - Data poisoning<br>• 2.4.4 - Broken access control<br>• 2.4.5 - Cryptographic failures<br>• 2.4.6 - Injection flaws<br>• 2.4.7 - Cross-site request forgery<br>• 2.4.8 - Directory traversal<br>• 2.4.10 - Security misconfiguration<br>• 2.4.12 - Identification and authentication failures<br>• 2.4.16 - Local file inclusion (LFI)/remote file inclusion (RFI)<br>2.5 Explain concepts related to vulnerability response, handling, and management<br>• 2.5.10 - Secure coding best practices<br>2.5.10.1 - Input validation |

| | | |
|---|---|---|
| 6.4 | SQL Injection | 2.2 Given a scenario, analyze output from vulnerability assessment tools<br>• 2.2.1 - Tools<br>2.2.1.2 - Web application scanners<br>2.2.1.2.1 - Burp Suite<br>2.4 Given a scenario, recommend controls to mitigate attacks and software vulnerabilities<br>• 2.4.6 - Injection flaws |
| 6.5 | Sniffing | 1.2 Given a scenario, analyze indicators of potentially malicious activity<br>• 1.2.1 - Network-related<br>1.3 Given a scenario, use appropriate tools or techniques to determine malicious activity<br>• 1.3.1 - Tools<br>1.3.1.1 - Packet capture<br>1.3.1.1.1 - Wireshark<br>1.3.1.1.2 - tcpdump<br>1.3.1.4 - Domain name service (DNS) and Internet Protocol (IP) reputation<br>2.2 Given a scenario, analyze output from vulnerability assessment tools<br>• 2.2.1 - Tools<br>2.2.1.1 - Network scanning and mapping |

| | | |
|---|---|---|
| 6.6 | Authentication Attacks | 1.1 Explain the importance of system and network architecture concepts in security operations<br>• 1.1.4 - Network architecture<br>1.1.4.2 - Cloud<br>1.2 Given a scenario, analyze indicators of potentially malicious activity<br>• 1.2.1 - Network-related<br>1.2.1.3 - Irregular peer-to-peer communication<br>1.2.1.5 - Scans/sweep<br>• 1.2.3 - Application-related<br>1.3 Given a scenario, use appropriate tools or techniques to determine malicious activity<br>• 1.3.1 - Tools<br>1.3.1.1.1 - Wireshark<br>1.3.1.4 - Domain name service (DNS) and Internet Protocol (IP) reputation<br>1.4 Compare and contrast threat-intelligence and threat-hunting concepts<br>• 1.4.6 - Threat hunting<br>1.4.6.1 - Indicators of compromise (IoC)<br>2.2 Given a scenario, analyze output from vulnerability assessment tools<br>• 2.2.1 - Tools |

| | | |
|---|---|---|
| | | 2.2.1.1 - Network scanning and mapping<br>2.4 Given a scenario, recommend controls to mitigate attacks and software vulnerabilities<br>• 2.4.1 - Cross-site scripting<br>• 2.4.3 - Data poisoning<br>• 2.4.4 - Broken access control<br>• 2.4.12 - Identification and authentication failures<br>2.5 Explain concepts related to vulnerability response, handling, and management<br>• 2.5.10 - Secure coding best practices<br>2.5.10.3 - Session management |
| 6.7 | Cloud Security | 1.1 Explain the importance of system and network architecture concepts in security operations<br>• 1.1.4 - Network architecture<br>1.1.4.2 - Cloud<br>1.2 Given a scenario, analyze indicators of potentially malicious activity<br>• 1.2.2 - Host-related<br>1.2.2.8 - Data exfiltration<br>2.1 Given a scenario, implement vulnerability scanning methods and concepts |

| | | |
|---|---|---|
| | | • 2.1.6 - Passive vs. active<br>2.2 Given a scenario, analyze output from vulnerability assessment tools<br>• 2.2.1 - Tools<br>2.2.1.6 - Cloud infrastructure assessment tools<br>2.2.1.6.1 - Scout Suite<br>2.2.1.6.2 - Prowler<br>2.2.1.6.3 - Pacu<br>2.5 Explain concepts related to vulnerability response, handling, and management<br>• 2.5.2 - Control types<br>2.5.2.1 - Managerial<br>2.5.2.2 - Operational<br>2.5.2.3 - Technical<br>2.5.2.4 - Preventative<br>2.5.2.5 - Detective<br>2.5.2.6 - Responsive<br>2.5.2.7 - Corrective |
| 6.8 | Email Security | 1.3 Given a scenario, use appropriate tools or techniques to determine malicious activity<br>• 1.3.2 - Common techniques<br>1.3.2.3 - Email analysis<br>1.3.2.3.1 - Header<br>1.3.2.3.2 - Impersonation<br>1.3.2.3.3 - DomainKeys Identified Mail (DKIM)<br>1.3.2.3.4 - Domain-based Message Authentication, Reporting, and Conformance (DMARC)<br>1.3.2.3.5 - Sender Policy Framework (SPF) |

| | | |
|---|---|---|
| | | 1.3.2.3.6 - Embedded links |
| 6.9 | Denial-of-Service Attacks | 1.2 Given a scenario, analyze indicators of potentially malicious activity<br>• 1.2.1 - Network-related<br>1.2.1.1 - Bandwidth consumption<br>1.3 Given a scenario, use appropriate tools or techniques to determine malicious activity<br>• 1.3.1 - Tools<br>1.3.1.1.1 - Wireshark<br>1.3.1.4 - Domain name service (DNS) and Internet Protocol (IP) reputation<br>2.2 Given a scenario, analyze output from vulnerability assessment tools<br>• 2.2.1 - Tools<br>2.2.1.1 - Network scanning and mapping<br>2.4 Given a scenario, recommend controls to mitigate attacks and software vulnerabilities<br>• 2.4.2 - Overflow vulnerabilities |
| 6.10 | Industrial Computer Systems | 2.1 Given a scenario, implement vulnerability scanning methods and concepts<br>• 2.1.8 - Critical infrastructure<br>2.1.8.1 - Operational technology (OT)<br>2.1.8.2 - Industrial control systems (ICS) |

| | | |
|---|---|---|
| | | 2.1.8.3 - Supervisory control and data acquisition (SCADA) |
| **7.0** | **Host-Based Attacks** | |
| 7.1 | Device Security | 1.1 Explain the importance of system and network architecture concepts in security operations<br>• 1.1.2 - Operating system (OS) concepts<br>1.1.2.2 - System hardening<br>• 1.1.6 - Encryption<br>1.2 Given a scenario, analyze indicators of potentially malicious activity<br>• 1.2.2 - Host-related<br>1.2.2.1 - Processor consumption<br>1.2.2.2 - Memory consumption<br>1.2.2.10 - File system changes or anomalies<br>1.3 Given a scenario, use appropriate tools or techniques to determine malicious activity<br>• 1.3.1 - Tools<br>1.3.1.3 - Endpoint security<br>1.3.1.5 - File analysis<br>• 1.3.2 - Common techniques<br>1.3.2.4 - File analysis<br>1.3.2.4.1 - Hashing |

| | | |
|---|---|---|
| | | 2.5 Explain concepts related to vulnerability response, handling, and management<br>• 2.5.7 - Policies, governance, and service-level objectives (SLOs)<br>3.2 Given a scenario, perform incident response activities<br>• 3.2.1 - Detection and analysis<br>• 3.2.2 - Containment, eradication, and recovery<br>3.3 Explain the preparation and post-incident activity phases of the incident management life cycle<br>• 3.3.2 - Post-incident activity<br>3.3.2.1 - Forensic analysis |
| 7.2 | Unauthorized Changes | 1.1 Explain the importance of system and network architecture concepts in security operations<br>• 1.1.2 - Operating system (OS) concepts<br>1.1.2.4 - System processes<br>1.2 Given a scenario, analyze indicators of potentially malicious activity<br>• 1.2.2 - Host-related<br>1.2.2.6 - Unauthorized changes<br>1.2.2.7 - Unauthorized privileges<br>1.2.2.9 - Abnormal OS process behavior<br>• 1.2.3 - Application-related |

| | | |
|---|---|---|
| | | 1.2.3.2 - Introduction of new accounts<br>1.3 Given a scenario, use appropriate tools or techniques to determine malicious activity<br>• 1.3.1 - Tools<br>1.3.1.2 - Log analysis/correlation<br>• 1.3.2 - Common techniques<br>1.3.2.5.1 - Abnormal account activity<br>2.4 Given a scenario, recommend controls to mitigate attacks and software vulnerabilities<br>• 2.4.12 - Identification and authentication failures<br>• 2.4.15 - Privilege escalation<br>3.2 Given a scenario, perform incident response activities<br>• 3.2.1 - Detection and analysis<br>3.2.1.3 - Data and log analysis |
| 7.3 | Malware | 1.1 Explain the importance of system and network architecture concepts in security operations<br>• 1.1.2 - Operating system (OS) concepts<br>1.1.2.1 - Windows Registry |

| | | |
|---|---|---|
| | | 1.2 Given a scenario, analyze indicators of potentially malicious activity<br>• 1.2.1 - Network-related<br>• 1.2.2 - Host-related<br>1.2.2.2 - Memory consumption<br>1.2.2.5 - Malicious processes<br>1.2.2.10 - File system changes or anomalies<br>• 1.2.3 - Application-related<br>• 1.2.4 - Other<br>1.2.4.2 - Obfuscated links<br>1.3 Given a scenario, use appropriate tools or techniques to determine malicious activity<br>• 1.3.1 - Tools<br>1.3.1.3 - Endpoint security<br>1.3.1.5.1 - Strings<br>1.3.1.6 - Sandboxing<br>1.4 Compare and contrast threat-intelligence and threat-hunting concepts<br>• 1.4.6 - Threat hunting<br>1.4.6.1 - Indicators of compromise (IoC)<br>1.4.6.1.1 - Collection<br>1.4.6.1.2 - Analysis<br>1.4.6.1.3 - Application<br>2.1 Given a scenario, implement vulnerability scanning methods and concepts |

| | | |
|---|---|---|
| | | • 2.1.1 - Asset discovery<br>2.1.1.2 - Device fingerprinting<br>• 2.1.7 - Static vs. dynamic<br>2.1.7.1 - Reverse engineering<br>2.1.7.2 - Fuzzing<br>2.4 Given a scenario, recommend controls to mitigate attacks and software vulnerabilities<br>• 2.4.4 - Broken access control<br>2.5 Explain concepts related to vulnerability response, handling, and management<br>• 2.5.3 - Patching and configuration management<br>4.1 Explain the importance of vulnerability management reporting and communication<br>• 4.1.3 - Action plans<br>4.1.3.4 - Awareness, education, and training |
| 7.4 | Command and Control | 1.2 Given a scenario, analyze indicators of potentially malicious activity<br>• 1.2.1 - Network-related<br>1.2.1.2 - Beaconing<br>2.2 Given a scenario, analyze output from vulnerability assessment tools<br>• 2.2.1 - Tools |

| | | |
|---|---|---|
| | | 2.2.1.1 - Network scanning and mapping |
| 7.5 | Social Engineering | 1.2 Given a scenario, analyze indicators of potentially malicious activity<br>• 1.2.4 - Other<br>1.2.4.1 - Social engineering attacks<br>1.2.4.2 - Obfuscated links<br>2.2 Given a scenario, analyze output from vulnerability assessment tools<br>• 2.2.1 - Tools<br>2.2.1.1 - Network scanning and mapping |
| 7.6 | Scripting and Programming | 1.3 Given a scenario, use appropriate tools or techniques to determine malicious activity<br>• 1.3.3 - Programming languages/scripting<br>1.3.3.1 - JavaScript Object Notation (JSON)<br>1.3.3.2 - Extensible Markup Language (XML)<br>1.3.3.3 - Python<br>1.3.3.4 - PowerShell<br>1.3.3.5 - Shell script<br>1.3.3.6 - Regular expressions<br>2.1 Given a scenario, implement vulnerability scanning methods and concepts<br>• 2.1.7 - Static vs. dynamic<br>2.1.7.1 - Reverse engineering |

| | | |
|---|---|---|
| | | 2.5 Explain concepts related to vulnerability response, handling, and management<br>• 2.5.10 - Secure coding best practices<br>2.5.10.1 - Input validation<br>2.5.10.2 - Output encoding<br>2.5.10.3 - Session management<br>2.5.10.4 - Authentication<br>2.5.10.5 - Data protection<br>2.5.10.6 - Parameterized queries<br>• 2.5.11 - Secure software development life cycle (SDLC) |
| 7.7 | Application Vulnerabilities | 2.4 Given a scenario, recommend controls to mitigate attacks and software vulnerabilities<br>• 2.4.1 - Cross-site scripting<br>• 2.4.2 - Overflow vulnerabilities<br>2.4.2.1 - Buffer<br>2.4.2.2 - Integer<br>2.4.2.3 - Heap<br>2.4.2.4 - Stack<br>• 2.4.4 - Broken access control<br>• 2.4.5 - Cryptographic failures<br>• 2.4.9 - Insecure design<br>• 2.4.10 - Security misconfiguration<br>• 2.4.11 - End-of-life or outdated components<br>• 2.4.12 - Identification and authentication failures<br>• 2.4.14 - Remote code execution |

| | | |
|---|---|---|
| | | • 2.4.15 - Privilege escalation |
| **8.0** | **Security Management** | |
| 8.1 | Security Information and Event Management (SIEM) | 1.2 Given a scenario, analyze indicators of potentially malicious activity<br>• 1.2.1 - Network-related<br>1.3 Given a scenario, use appropriate tools or techniques to determine malicious activity<br>• 1.3.1 - Tools<br>1.3.1.2 - Log analysis/correlation<br>1.3.1.2.1 - Security information and event management (SIEM)<br>2.2 Given a scenario, analyze output from vulnerability assessment tools<br>• 2.2.1 - Tools<br>2.2.1.1 - Network scanning and mapping |
| 8.2 | Security Orchestration, Automation, and Response (SOAR) | 1.2 Given a scenario, analyze indicators of potentially malicious activity<br>• 1.2.2 - Host-related<br>1.2.2.5 - Malicious processes<br>1.3 Given a scenario, use appropriate tools or techniques to determine malicious activity<br>• 1.3.1 - Tools |

| | | |
|---|---|---|
| | | 1.3.1.2.2 - Security orchestration, automation, and response (SOAR)<br>• 1.3.3 - Programming languages/scripting<br>1.5 Explain the importance of efficiency and process improvement in security operations<br>• 1.5.1 - Standardize processes<br>1.5.1.1 - Identification of tasks suitable for automation<br>1.5.1.2 - Team coordination to manage and facilitate automation<br>• 1.5.2 - Streamline operations<br>1.5.2.1 - Automation and orchestration<br>1.5.2.2 - Orchestrating threat intelligence data<br>1.5.2.2.2 - Threat feed combination<br>• 1.5.3 - Technology and tool integration<br>1.5.3.1 - Application programming interface (API)<br>• 1.5.4 - Single pane of glass<br>3.2 Given a scenario, perform incident response activities<br>• 3.2.1 - Detection and analysis<br>3.2.1.3 - Data and log analysis |
| 8.3 | Exploring Abnormal Activity | 1.2 Given a scenario, analyze indicators of potentially malicious activity<br>• 1.2.1 - Network-related |

| | | |
|---|---|---|
| | | 1.2.1.3 - Irregular peer-to-peer communication<br>1.2.1.7 - Activity on unexpected ports<br>• 1.2.3 - Application-related<br>1.2.3.1 - Anomalous activity<br>1.2.3.4 - Unexpected outbound communication<br>1.2.3.5 - Service interruption<br>1.2.3.6 - Application logs<br>1.3 Given a scenario, use appropriate tools or techniques to determine malicious activity<br>• 1.3.1 - Tools<br>1.3.1.1.1 - Wireshark<br>1.3.1.2.1 - Security information and event management (SIEM)<br>1.3.1.3 - Endpoint security<br>1.3.1.3.1 - Endpoint detection and response (EDR)<br>1.3.1.4 - Domain name service (DNS) and Internet Protocol (IP) reputation<br>• 1.3.2 - Common techniques<br>1.3.2.2 - Interpreting suspicious commands<br>1.3.2.4 - File analysis<br>1.3.2.5.1 - Abnormal account activity<br>• 1.3.3 - Programming languages/scripting<br>1.3.3.4 - PowerShell<br>1.3.3.5 - Shell script |
| **9.0** | **Post-Attack** | |

| | | |
|---|---|---|
| 9.1 | Containment | 1.4 Compare and contrast threat-intelligence and threat-hunting concepts<br>• 1.4.6 - Threat hunting<br>1.4.6.2.2 - Isolated networks<br>2.4 Given a scenario, recommend controls to mitigate attacks and software vulnerabilities<br>• 2.4.5 - Cryptographic failures<br>3.2 Given a scenario, perform incident response activities<br>• 3.2.1 - Detection and analysis<br>3.2.1.2 - Evidence acquisitions<br>• 3.2.2 - Containment, eradication, and recovery<br>3.2.2.1 - Scope<br>3.2.2.2 - Impact<br>3.2.2.3 - Isolation<br>3.2.2.4 - Remediation<br>3.2.2.5 - Re-imaging<br>3.2.2.6 - Compensating controls<br>3.3 Explain the preparation and post-incident activity phases of the incident management life cycle<br>• 3.3.2 - Post-incident activity<br>3.3.2.1 - Forensic analysis |
| 9.2 | Incident Response | 1.2 Given a scenario, analyze indicators of potentially malicious activity |

| | | |
|---|---|---|
| | | • 1.2.2 - Host-related<br>1.2.2.8 - Data exfiltration<br>• 1.2.4 - Other<br>1.2.4.1 - Social engineering attacks<br>1.3 Given a scenario, use appropriate tools or techniques to determine malicious activity<br>• 1.3.1 - Tools<br>1.3.1.2.1 - Security information and event management (SIEM)<br>1.4 Compare and contrast threat-intelligence and threat-hunting concepts<br>• 1.4.5 - Threat intelligence sharing<br>1.4.5.1 - Incident response<br>2.5 Explain concepts related to vulnerability response, handling, and management<br>• 2.5.9 - Attack surface management<br>2.5.9.4 - Penetration testing and adversary emulation<br>3.2 Given a scenario, perform incident response activities<br>• 3.2.1 - Detection and analysis<br>3.2.1.1 - IoC<br>3.2.1.2.1 - Chain of custody<br>3.2.1.3 - Data and log analysis |

| | | |
|---|---|---|
| | | • 3.2.2 - Containment, eradication, and recovery<br>3.2.2.1 - Scope<br>3.2.2.2 - Impact<br>3.3 Explain the preparation and post-incident activity phases of the incident management life cycle<br>• 3.3.1 - Preparation<br>3.3.1.1 - Incident response plan<br>3.3.1.2 - Tools<br>3.3.1.3 - Playbooks<br>3.3.1.4 - Tabletop<br>3.3.1.5 - Training<br>3.3.1.6 - Business continuity (BC)/ disaster recovery (DR)<br>• 3.3.2 - Post-incident activity<br>3.3.2.3 - Lessons learned<br>4.1 Explain the importance of vulnerability management reporting and communication<br>• 4.1.6 - Stakeholder identification and communication<br>4.2 Explain the importance of incident response reporting and communication<br>• 4.2.2 - Incident declaration and escalation<br>• 4.2.3 - Incident response reporting<br>• 4.2.4 - Communications<br>4.2.4.1 - Legal<br>4.2.4.2 - Public relations<br>4.2.4.2.1 - Customer communication |

| | | |
|---|---|---|
| | | 4.2.4.2.2 - Media<br>4.2.4.3 - Regulatory reporting<br>4.2.4.4 - Law enforcement |
| 9.3 | Post-Incident Activities | 1.1 Explain the importance of system and network architecture concepts in security operations<br>• 1.1.3 - Infrastructure concepts<br>1.1.3.2 - Virtualization<br>1.3 Given a scenario, use appropriate tools or techniques to determine malicious activity<br>• 1.3.2 - Common techniques<br>1.3.2.4.1 - Hashing<br>2.1 Given a scenario, implement vulnerability scanning methods and concepts<br>• 2.1.8 - Critical infrastructure<br>2.1.8.3 - Supervisory control and data acquisition (SCADA)<br>3.2 Given a scenario, perform incident response activities<br>• 3.2.1 - Detection and analysis<br>3.2.1.2 - Evidence acquisitions<br>3.2.1.2.1 - Chain of custody<br>3.2.1.2.4 - Legal hold<br>3.3 Explain the preparation and post-incident activity phases of the incident management life cycle |

| | | |
|---|---|---|
| | | • 3.3.1 - Preparation<br>3.3.1.6 - Business continuity (BC)/ disaster recovery (DR)<br>• 3.3.2 - Post-incident activity<br>3.3.2.1 - Forensic analysis<br>4.2 Explain the importance of incident response reporting and communication<br>• 4.2.2 - Incident declaration and escalation<br>• 4.2.3 - Incident response reporting<br>4.2.3.1 - Executive summary<br>4.2.3.2 - Who, what, when, where, and why<br>4.2.3.3 - Recommendations<br>4.2.3.7 - Evidence<br>• 4.2.5 - Root cause analysis<br>• 4.2.6 - Lessons learned<br>• 4.2.7 - Metrics and KPIs<br>4.2.7.1 - Mean time to detect<br>4.2.7.2 - Mean time to respond<br>4.2.7.3 - Mean time to remediate |
| **A.0** | **CompTIA CySA+ CS0-003 - Practice Exams** | |
| A.1 | Prepare for CompTIA CySA+ Certification | |

| | | |
|---|---|---|
| A.2 | CompTIA CySA+ CS0-003 Domain Review (20 Questions) | |
| A.3 | CompTIA CySA+ CS0-003 Practice Exams (All Questions) | |
| **B.0** | **TestOut CyberDefense Pro - Practice Exams** | |
| B.1 | Prepare for TestOut CyberDefense Pro Certification | |
| B.2 | TestOut CyberDefense Pro Exam Domain Review | |

## **Objective Mapping:** CompTIA CySA+ CS0-003 Objective to LabSim Section

| # | Domain | Module.Section |
|---|---|---|
| **1.0** | **Security Operations** | |
| 1.1 | Explain the importance of system and network architecture concepts in security operations<br>1.1.1 - Log ingestion<br>○ 1.1.1.1 - Time synchronization<br>○ 1.1.1.2 - Logging levels<br>1.1.2 - Operating system (OS) concepts<br>○ 1.1.2.1 - Windows Registry<br>○ 1.1.2.2 - System hardening<br>○ 1.1.2.3 - File structure<br>○ 1.1.2.3.1 - Configuration file locations<br>○ 1.1.2.4 - System processes<br>○ 1.1.2.5 - Hardware architecture<br>1.1.3 - Infrastructure concepts<br>○ 1.1.3.1 - Serverless<br>○ 1.1.3.2 - Virtualization<br>○ 1.1.3.3 - Containerization<br>1.1.4 - Network architecture<br>○ 1.1.4.1 - On-premises<br>○ 1.1.4.2 - Cloud<br>○ 1.1.4.3 - Hybrid<br>○ 1.1.4.4 - Network segmentation<br>○ 1.1.4.5 - Zero trust<br>○ 1.1.4.6 - Secure access secure edge (SASE)<br>○ 1.1.4.7 - Software-defined networking (SDN)<br>1.1.5 - Identity and access management<br>○ 1.1.5.1 - Multifactor authentication (MFA)<br>○ 1.1.5.2 - Single sign-on (SSO)<br>○ 1.1.5.3 - Federation<br>○ 1.1.5.4 - Privileged access management (PAM)<br>○ 1.1.5.5 - Passwordless<br>○ 1.1.5.6 - Cloud access security broker (CASB)<br>1.1.6 - Encryption | 4.1, 4.2, 4.3, 4.4, 4.5<br>5.1, 5.2<br>6.6, 6.7<br>7.1, 7.2, 7.3<br>9.3 |

| | | |
|---|---|---|
| | ○ 1.1.6.1 - Public key infrastructure (PKI)<br>○ 1.1.6.2 - Secure sockets layer (SSL) inspection<br>1.1.7 - Sensitive data protection<br>○ 1.1.7.1 - Data loss prevention (DLP)<br>○ 1.1.7.2 - Personally identifiable information (PII)<br>○ 1.1.7.3 - Cardholder data (CHD) | |
| 1.2 | Given a scenario, analyze indicators of potentially malicious activity<br>1.2.1 - Network-related<br>○ 1.2.1.1 - Bandwidth consumption<br>○ 1.2.1.2 - Beaconing<br>○ 1.2.1.3 - Irregular peer-to-peer communication<br>○ 1.2.1.4 - Rogue devices on the network<br>○ 1.2.1.5 - Scans/sweep<br>○ 1.2.1.6 - Unusual traffic spikes<br>○ 1.2.1.7 - Activity on unexpected ports<br>1.2.2 - Host-related<br>○ 1.2.2.1 - Processor consumption<br>○ 1.2.2.2 - Memory consumption<br>○ 1.2.2.3 - Drive capacity consumption<br>○ 1.2.2.4 - Unauthorized software<br>○ 1.2.2.5 - Malicious processes<br>○ 1.2.2.6 - Unauthorized changes<br>○ 1.2.2.7 - Unauthorized privileges<br>○ 1.2.2.8 - Data exfiltration<br>○ 1.2.2.9 - Abnormal OS process behavior<br>○ 1.2.2.10 - File system changes or anomalies<br>○ 1.2.2.11 - Registry changes or anomalies<br>○ 1.2.2.12 - Unauthorized scheduled tasks<br>1.2.3 - Application-related<br>○ 1.2.3.1 - Anomalous activity<br>○ 1.2.3.2 - Introduction of new accounts<br>○ 1.2.3.3 - Unexpected output<br>○ 1.2.3.4 - Unexpected outbound communication<br>○ 1.2.3.5 - Service interruption<br>○ 1.2.3.6 - Application logs<br>1.2.4 - Other | 3.2, 3.3, 3.4<br>4.1, 4.4, 4.5<br>5.1, 5.2<br>6.1, 6.2, 6.3, 6.5, 6.6, 6.7, 6.9<br>7.1, 7.2, 7.3, 7.4, 7.5<br>8.1, 8.2, 8.3<br>9.2 |

| | | |
|---|---|---|
| | ○ 1.2.4.1 - Social engineering attacks<br>○ 1.2.4.2 - Obfuscated links | |
| 1.3 | Given a scenario, use appropriate tools or techniques to determine malicious activity<br>1.3.1 - Tools<br>○ 1.3.1.1 - Packet capture<br>○ 1.3.1.1.1 - Wireshark<br>○ 1.3.1.1.2 - tcpdump<br>○ 1.3.1.2 - Log analysis/correlation<br>○ 1.3.1.2.1 - Security information and event management (SIEM)<br>○ 1.3.1.2.2 - Security orchestration, automation, and response (SOAR)<br>○ 1.3.1.3 - Endpoint security<br>○ 1.3.1.3.1 - Endpoint detection and response (EDR)<br>○ 1.3.1.4 - Domain name service (DNS) and Internet Protocol (IP) reputation<br>○ 1.3.1.4.1 - WHOIS<br>○ 1.3.1.4.2 - AbuseIPDB<br>○ 1.3.1.5 - File analysis<br>○ 1.3.1.5.1 - Strings<br>○ 1.3.1.5.2 - VirusTotal<br>○ 1.3.1.6 - Sandboxing<br>○ 1.3.1.6.1 - Joe Sandbox<br>○ 1.3.1.6.2 - Cuckoo Sandbox<br>1.3.2 - Common techniques<br>○ 1.3.2.1 - Pattern recognition<br>○ 1.3.2.1.1 - Command and control<br>○ 1.3.2.2 - Interpreting suspicious commands<br>○ 1.3.2.3 - Email analysis<br>○ 1.3.2.3.1 - Header<br>○ 1.3.2.3.2 - Impersonation<br>○ 1.3.2.3.3 - DomainKeys Identified Mail (DKIM)<br>○ 1.3.2.3.4 - Domain-based Message Authentication, Reporting, and Conformance (DMARC)<br>○ 1.3.2.3.5 - Sender Policy Framework (SPF)<br>○ 1.3.2.3.6 - Embedded links<br>○ 1.3.2.4 - File analysis<br>○ 1.3.2.4.1 - Hashing<br>○ 1.3.2.5 - User behavior analysis | 4.4, 4.5<br>5.1<br>6.3, 6.5, 6.6, 6.8, 6.9<br>7.1, 7.2, 7.3, 7.6<br>8.1, 8.2, 8.3<br>9.2, 9.3 |

| | | |
|---|---|---|
| | ○ 1.3.2.5.1 - Abnormal account activity<br>○ 1.3.2.5.2 - Impossible travel<br>1.3.3 - Programming languages/scripting<br>○ 1.3.3.1 - JavaScript Object Notation (JSON)<br>○ 1.3.3.2 - Extensible Markup Language (XML)<br>○ 1.3.3.3 - Python<br>○ 1.3.3.4 - PowerShell<br>○ 1.3.3.5 - Shell script<br>○ 1.3.3.6 - Regular expressions | |
| 1.4 | Compare and contrast threat-intelligence and threat-hunting concepts<br>1.4.1 - Threat actors<br>○ 1.4.1.1 - Advanced persistent threat (APT)<br>○ 1.4.1.2 - Hacktivists<br>○ 1.4.1.3 - Organized crime<br>○ 1.4.1.4 - Nation-state<br>○ 1.4.1.5 - Script kiddie<br>○ 1.4.1.6 - Insider threat<br>○ 1.4.1.6.1 - Intentional<br>○ 1.4.1.6.2 - Unintentional<br>○ 1.4.1.7 - Supply chain<br>1.4.2 - Tactics, techniques, and procedures (TTP)<br>1.4.3 - Confidence levels<br>○ 1.4.3.1 - Timeliness<br>○ 1.4.3.2 - Relevancy<br>○ 1.4.3.3 - Accuracy<br>1.4.4 - Collection methods and sources<br>○ 1.4.4.1 - Open source<br>○ 1.4.4.1.1 - Social media<br>○ 1.4.4.1.2 - Blogs/forums<br>○ 1.4.4.1.3 - Government bulletins<br>○ 1.4.4.1.4 - Computer emergency response team (CERT)<br>○ 1.4.4.1.5 - Cybersecurity incident response team (CSIRT)<br>○ 1.4.4.1.6 - Deep/dark web<br>○ 1.4.4.2 - Closed source<br>○ 1.4.4.2.1 - Paid feeds<br>○ 1.4.4.2.2 - Information sharing organizations | 2.2, 2.4, 2.6<br>3.1, 3.2, 3.3, 3.4<br>4.2, 4.4<br>5.2, 5.5, 5.6<br>6.1, 6.6<br>7.3<br>9.1, 9.2 |

| | | |
|---|---|---|
| | ○ 1.4.4.2.3 - Internal sources<br>1.4.5 - Threat intelligence sharing<br>○ 1.4.5.1 - Incident response<br>○ 1.4.5.2 - Vulnerability management<br>○ 1.4.5.3 - Risk management<br>○ 1.4.5.4 - Security engineering<br>○ 1.4.5.5 - Detection and monitoring<br>1.4.6 - Threat hunting<br>○ 1.4.6.1 - Indicators of compromise (IoC)<br>○ 1.4.6.1.1 - Collection<br>○ 1.4.6.1.2 - Analysis<br>○ 1.4.6.1.3 - Application<br>○ 1.4.6.2 - Focus areas<br>○ 1.4.6.2.1 - Configurations/ misconfigurations<br>○ 1.4.6.2.2 - Isolated networks<br>○ 1.4.6.2.3 - Business-critical assets and processes<br>○ 1.4.6.3 - Active defense<br>○ 1.4.6.4 - Honeypot | |
| 1.5 | Explain the importance of efficiency and process improvement in security operations<br>1.5.1 - Standardize processes<br>○ 1.5.1.1 - Identification of tasks suitable for automation<br>○ 1.5.1.1.1 - Repeatable/do not require human interaction<br>○ 1.5.1.2 - Team coordination to manage and facilitate automation<br>1.5.2 - Streamline operations<br>○ 1.5.2.1 - Automation and orchestration<br>○ 1.5.2.1.1 - Security orchestration, automation, and response (SOAR)<br>○ 1.5.2.2 - Orchestrating threat intelligence data<br>○ 1.5.2.2.1 - Data enrichment<br>○ 1.5.2.2.2 - Threat feed combination<br>○ 1.5.2.3 - Minimize human engagement<br>1.5.3 - Technology and tool integration<br>○ 1.5.3.1 - Application programming interface (API)<br>○ 1.5.3.2 - Webhooks<br>○ 1.5.3.3 - Plugins<br>1.5.4 - Single pane of glass | 3.3<br>8.2 |

| **2.0** | **Vulnerability Management** | |
|---|---|---|
| 2.1 | Given a scenario, implement vulnerability scanning methods and concepts<br>2.1.1 - Asset discovery<br>○ 2.1.1.1 - Map scans<br>○ 2.1.1.2 - Device fingerprinting<br>2.1.2 - Special considerations<br>○ 2.1.2.1 - Scheduling<br>○ 2.1.2.2 - Operations<br>○ 2.1.2.3 - Performance<br>○ 2.1.2.4 - Sensitivity levels<br>○ 2.1.2.5 - Segmentation<br>○ 2.1.2.6 - Regulatory requirements<br>2.1.3 - Internal vs. external scanning<br>2.1.4 - Agent vs. agentless<br>2.1.5 - Credentialed vs. non-credentialed<br>2.1.6 - Passive vs. active<br>2.1.7 - Static vs. dynamic<br>○ 2.1.7.1 - Reverse engineering<br>○ 2.1.7.2 - Fuzzing<br>2.1.8 - Critical infrastructure<br>○ 2.1.8.1 - Operational technology (OT)<br>○ 2.1.8.2 - Industrial control systems (ICS)<br>○ 2.1.8.3 - Supervisory control and data acquisition (SCADA)<br>2.1.9 - Security baseline scanning<br>2.1.10 - Industry frameworks<br>○ 2.1.10.1 - Payment Card Industry Data Security Standard (PCI DSS)<br>○ 2.1.10.2 - Center for Internet Security (CIS) benchmarks<br>○ 2.1.10.3 - Open Web Application Security Project (OWASP)<br>○ 2.1.10.4 - International Organization for Standardization (ISO) 27000 series | 2.1, 2.3<br>3.2, 3.4<br>4.1, 4.4<br>5.1, 5.2, 5.3, 5.4, 5.6<br>6.1, 6.7, 6.10<br>7.3, 7.6<br>9.3 |
| 2.2 | Given a scenario, analyze output from vulnerability assessment tools<br>2.2.1 - Tools<br>○ 2.2.1.1 - Network scanning and mapping<br>○ 2.2.1.1.1 - Angry IP Scanner | 3.4<br>4.1<br>5.1, 5.2, 5.3, 5.4, 5.5 |

| | | |
|---|---|---|
| | o 2.2.1.1.2 - Maltego<br>o 2.2.1.2 - Web application scanners<br>o 2.2.1.2.1 - Burp Suite<br>o 2.2.1.2.2 - Zed Attack Proxy (ZAP)<br>o 2.2.1.2.3 - Arachni<br>o 2.2.1.2.4 - Nikto<br>o 2.2.1.3 - Vulnerability scanners<br>o 2.2.1.3.1 - Nessus<br>o 2.2.1.3.2 - OpenVAS<br>o 2.2.1.4 - Debuggers<br>o 2.2.1.4.1 - Immunity debugger<br>o 2.2.1.4.2 - GNU debugger (GDB)<br>o 2.2.1.5 - Multipurpose<br>o 2.2.1.5.1 - Nmap<br>o 2.2.1.5.2 - Metasploit framework (MSF)<br>o 2.2.1.5.3 - Recon-ng<br>o 2.2.1.6 - Cloud infrastructure assessment tools<br>o 2.2.1.6.1 - Scout Suite<br>o 2.2.1.6.2 - Prowler<br>o 2.2.1.6.3 - Pacu | 6.1, 6.3, 6.4, 6.5, 6.6, 6.7, 6.9<br>7.4, 7.5<br>8.1 |
| 2.3 | Given a scenario, analyze data to prioritize vulnerabilities<br>2.3.1 - Common Vulnerability Scoring System (CVSS) interpretation<br>o 2.3.1.1 - Attack vectors<br>o 2.3.1.2 - Attack complexity<br>o 2.3.1.3 - Privileges required<br>o 2.3.1.4 - User interaction<br>o 2.3.1.5 - Scope<br>o 2.3.1.6 - Impact<br>o 2.3.1.6.1 - Confidentiality<br>o 2.3.1.6.2 - Integrity<br>o 2.3.1.6.3 - Availability<br>2.3.2 - Validation<br>o 2.3.2.1 - True/false positives<br>o 2.3.2.2 - True/false negatives<br>2.3.3 - Context awareness<br>o 2.3.3.1 - Internal | 3.4<br>4.4<br>5.2, 5.4, 5.5, 5.6 |

| | | |
|---|---|---|
| | ○ 2.3.3.2 - External<br>○ 2.3.3.3 - Isolated<br>2.3.4 - Exploitability/weaponization<br>2.3.5 - Asset value<br>2.3.6 - Zero-day | |
| 2.4 | Given a scenario, recommend controls to mitigate attacks and software vulnerabilities<br>2.4.1 - Cross-site scripting<br>○ 2.4.1.1 - Reflected<br>○ 2.4.1.2 - Persistent<br>2.4.2 - Overflow vulnerabilities<br>○ 2.4.2.1 - Buffer<br>○ 2.4.2.2 - Integer<br>○ 2.4.2.3 - Heap<br>○ 2.4.2.4 - Stack<br>2.4.3 - Data poisoning<br>2.4.4 - Broken access control<br>2.4.5 - Cryptographic failures<br>2.4.6 - Injection flaws<br>2.4.7 - Cross-site request forgery<br>2.4.8 - Directory traversal<br>2.4.9 - Insecure design<br>2.4.10 - Security misconfiguration<br>2.4.11 - End-of-life or outdated components<br>2.4.12 - Identification and authentication failures<br>2.4.13 - Server-side request forgery<br>2.4.14 - Remote code execution<br>2.4.15 - Privilege escalation<br>2.4.16 - Local file inclusion (LFI)/remote file inclusion (RFI) | 5.1, 5.3, 5.4<br>6.3, 6.4, 6.6, 6.9<br>7.2, 7.3, 7.7<br>9.1 |
| 2.5 | Explain concepts related to vulnerability response, handling, and management<br>2.5.1 - Compensating control<br>2.5.2 - Control types<br>○ 2.5.2.1 - Managerial<br>○ 2.5.2.2 - Operational | 2.1, 2.2, 2.3, 2.4, 2.5<br>3.3, 3.4<br>5.2, 5.3, 5.4, 5.6 |

| | | |
|---|---|---|
| | ○ 2.5.2.3 - Technical<br>○ 2.5.2.4 - Preventative<br>○ 2.5.2.5 - Detective<br>○ 2.5.2.6 - Responsive<br>○ 2.5.2.7 - Corrective<br>2.5.3 - Patching and configuration management<br>2.5.3.1 - Testing<br>2.5.3.2 - Implementation<br>2.5.3.3 - Rollback<br>2.5.3.4 - Validation<br>2.5.4 - Maintenance windows<br>2.5.5 - Exceptions<br>2.5.6 - Risk management principles<br>○ 2.5.6.1 - Accept<br>○ 2.5.6.2 - Transfer<br>○ 2.5.6.3 - Avoid<br>○ 2.5.6.4 - Mitigate<br>2.5.7 - Policies, governance, and service-level objectives (SLOs)<br>2.5.8 - Prioritization and escalation<br>2.5.9 - Attack surface management<br>○ 2.5.9.1 - Edge discovery<br>○ 2.5.9.2 - Passive discovery<br>○ 2.5.9.3 - Security controls testing<br>○ 2.5.9.4 - Penetration testing and adversary emulation<br>○ 2.5.9.5 - Bug bounty<br>○ 2.5.9.6 - Attack surface reduction<br>2.5.10 - Secure coding best practices<br>○ 2.5.10.1 - Input validation<br>○ 2.5.10.2 - Output encoding<br>○ 2.5.10.3 - Session management<br>○ 2.5.10.4 - Authentication<br>○ 2.5.10.5 - Data protection<br>○ 2.5.10.6 - Parameterized queries<br>2.5.11 - Secure software development life cycle (SDLC)<br>2.5.12 - Threat modeling | 6.3, 6.6, 6.7<br>7.1, 7.3, 7.6<br>9.2 |
| **3.0** | **Incident Response and Management** | |

| | | |
|---|---|---|
| 3.1 | Explain concepts related to attack methodology frameworks<br>3.1.1 - Cyber kill chain<br>○ 3.1.1.1 - Reconnaissance<br>○ 3.1.1.2 - Weaponization<br>○ 3.1.1.3 - Delivery<br>○ 3.1.1.4 - Exploitation<br>○ 3.1.1.5 - Installation<br>○ 3.1.1.6 - Command and Control (C2)<br>○ 3.1.1.7 - Actions and objectives<br>3.1.2 - Diamond Model of Intrusion Analysis<br>○ 3.1.2.1 - Adversary<br>○ 3.1.2.2 - Victim<br>○ 3.1.2.3 - Infrastructure<br>○ 3.1.2.4 - Capability<br>3.1.3 - MITRE ATT&CK<br>3.1.4 - Open Source Security Testing Methodology Manual (OSS TMM)<br>3.1.5 - OWASP Testing Guide | 2.6<br>3.3 |
| 3.2 | Given a scenario, perform incident response activities<br>3.2.1 - Detection and analysis<br>○ 3.2.1.1 - IoC<br>○ 3.2.1.2 - Evidence acquisitions<br>○ 3.2.1.2.1 - Chain of custody<br>○ 3.2.1.2.2 - Validating data integrity<br>○ 3.2.1.2.3 - Preservation<br>○ 3.2.1.2.4 - Legal hold<br>○ 3.2.1.3 - Data and log analysis<br>3.2.2 - Containment, eradication, and recovery<br>○ 3.2.2.1 - Scope<br>○ 3.2.2.2 - Impact<br>○ 3.2.2.3 - Isolation<br>○ 3.2.2.4 - Remediation<br>○ 3.2.2.5 - Re-imaging<br>○ 3.2.2.6 - Compensating controls | 3.3, 3.4<br>4.5<br>5.1, 5.2<br>6.1<br>7.1, 7.2<br>8.2<br>9.1, 9.2, 9.3 |

| | | |
|---|---|---|
| 3.3 | Explain the preparation and post-incident activity phases of the incident management life cycle<br>3.3.1 - Preparation<br>○ 3.3.1.1 - Incident response plan<br>○ 3.3.1.2 - Tools<br>○ 3.3.1.3 - Playbooks<br>○ 3.3.1.4 - Tabletop<br>○ 3.3.1.5 - Training<br>○ 3.3.1.6 - Business continuity (BC)/ disaster recovery (DR)<br>3.3.2 - Post-incident activity<br>○ 3.3.2.1 - Forensic analysis<br>○ 3.3.2.2 - Root cause analysis<br>○ 3.3.2.3 - Lessons learned | 3.3<br>7.1<br>9.1, 9.2, 9.3 |
| **4.0** | **Reporting and Communication** | |
| 4.1 | Explain the importance of vulnerability management reporting and communication<br>4.1.1 - Vulnerability management reporting<br>○ 4.1.1.1 - Vulnerabilities<br>○ 4.1.1.2 - Affected hosts<br>○ 4.1.1.3 - Risk score<br>○ 4.1.1.4 - Mitigation<br>○ 4.1.1.5 - Recurrence<br>○ 4.1.1.6 - Prioritization<br>4.1.2 - Compliance reports<br>4.1.3 - Action plans<br>○ 4.1.3.1 - Configuration management<br>○ 4.1.3.2 - Patching<br>○ 4.1.3.3 - Compensating controls<br>○ 4.1.3.4 - Awareness, education, and training<br>○ 4.1.3.5 - Changing business requirements<br>4.1.4 - Inhibitors to remediation<br>○ 4.1.4.1 - Memorandum of understanding (MOU)<br>○ 4.1.4.2 - Service-level agreement (SLA)<br>○ 4.1.4.3 - Organizational governance<br>○ 4.1.4.4 - Business process interruption | 2.1, 2.5<br>4.4<br>5.4, 5.5, 5.6<br>6.1<br>7.3<br>9.2 |

| | | |
|---|---|---|
| | ○ 4.1.4.5 - Degrading functionality<br>○ 4.1.4.6 - Legacy systems<br>○ 4.1.4.7 - Proprietary systems<br>4.1.5 - Metrics and key performance indicators (KPIs)<br>○ 4.1.5.1 - Trends<br>○ 4.1.5.2 - Top 10<br>○ 4.1.5.3 - Critical vulnerabilities and zero-days<br>○ 4.1.5.4 - SLOs<br>4.1.6 - Stakeholder identification and communication | |
| 4.2 | Explain the importance of incident response reporting and communication<br>4.2.1 - Stakeholder identification and communication<br>4.2.2 - Incident declaration and escalation<br>4.2.3 - Incident response reporting<br>○ 4.2.3.1 - Executive summary<br>○ 4.2.3.2 - Who, what, when, where, and why<br>○ 4.2.3.3 - Recommendations<br>○ 4.2.3.4 - Timeline<br>○ 4.2.3.5 - Impact<br>○ 4.2.3.6 - Scope<br>○ 4.2.3.7 - Evidence<br>4.2.4 - Communications<br>○ 4.2.4.1 - Legal<br>○ 4.2.4.2 - Public relations<br>○ 4.2.4.2.1 - Customer communication<br>○ 4.2.4.2.2 - Media<br>○ 4.2.4.3 - Regulatory reporting<br>○ 4.2.4.4 - Law enforcement<br>4.2.5 - Root cause analysis<br>4.2.6 - Lessons learned<br>4.2.7 - Metrics and KPIs<br>○ 4.2.7.1 - Mean time to detect<br>○ 4.2.7.2 - Mean time to respond<br>○ 4.2.7.3 - Mean time to remediate<br>○ 4.2.7.4 - Alert volume | 9.2, 9.3 |